

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**

IN THE MATTER OF THE SEARCH OF:  
All Content and Other Information Associated  
With iCloud Account nyree08@icloud.com  
Maintained at Premises Controlled by Apple, Inc.

Case No. 19 - 0973 JMC

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

I, Special Agent Erin Fuchs, being first duly sworn, hereby depose and say the following:

1. I am a duly sworn and appointed Special Agent of the United States Department of Health and Human Services, Office of Inspector General, Office of Investigations (hereinafter "HHS-OIG"). I have been a Special Agent since December of 2006 and am currently assigned to the Columbia Field Office where I conduct health care fraud investigations. I have training and experience in the enforcement of the laws of the United States, including training in the preparation, presentation, and service of criminal search warrants. I have duties that include investigations of, among other matters, health care fraud, wire fraud, and false claims. Through my training and my participation in searches and arrests, I have assisted and/or participated in the preparation and/or execution of search and arrest warrants. This affidavit does not set forth every fact discerned throughout the investigation; rather, it contains a summary of the investigation to date and sets forth only those facts that I believe necessary to establish probable cause to search the account described herein.

2. The facts in this affidavit come from information obtained from other agents and law enforcement officers, witnesses, my knowledge, training and experience, and personal observations. This affidavit is intended to show there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. I anticipate executing the requested warrant to search the SUBJECT ACCOUNT

**19 - 0973 JMC**

under the Electronic Communications Privacy Act, 18 U.S.C. § 2703, for all content and other information associated with the SUBJECT ACCOUNT; namely, iCloud Account nyree08@icloud.com, maintained at Premises Controlled by Apple, Inc.

4. Based on my knowledge, training and experience and the facts set forth in this affidavit, there is probable cause to believe that evidence, fruits and instrumentalities of violations of 18 U.S.C. § 1512(a) and (k) (Tampering with a Witness, Victim, or an Informant), 18 U.S.C. § 922/924(c) (Possession/Use of a Firearm/Ammunition in Furtherance of a Crime of Violence), and 21 U.S.C. § 841/846 (Possession with Intent to Distribute Marijuana and Conspiring to Possess with Intent to Distribute Marijuana) (“TARGET OFFENSES”) will be found in the SUBJECT ACCOUNT.

5. This warrant would require Apple to disclose to the government copies of the records and other information (including the content of communications), more fully described in Attachment B pertaining to the subscriber or customer associated with the account more fully described in Attachment A, stored at premises owned, maintained, controlled, or operated by Apple.

6. Apple Inc. (“Apple”) is an American multinational corporation that designs, develops, and sells consumer electronics, computer software and personal computers, including the iPhone, a “smart phone” with the capability to function as a telephone, image and video recording device, and includes many, if not all of, the capabilities of a desktop computer.

7. Apple, Inc., provides users with the ability to store files, photographs, and messages, on a drive that is housed on data servers not located on the users device. The user can capture the data on their computer or mobile device, then upload or sync the data to servers owned and operated by Apple, Inc. Once the data is uploaded or synched the user can remove the data from

*su*

19 - 0973 JMC

their computer or mobile device, but still be able to access data from any computer by logging onto their iCloud account. Apple, Inc., provides users with 5GB of free space upon signing up for iCloud services; however, the user can upgrade to as many as multiple terabytes of storage space for a monthly fee. Apple also provides its users with email addresses at domains including @icloud.com.

8. "iMessage" is an Apple propriety messaging platform which allows users of Apple devices to share text, image and video communications. Using the Messages application on any Apple device that uses Apple iOS, such as an iPhone, or Mac OS X, a user can send an iMessage to any other iOS or Mac OS X device. Further, iMessages sent from one Apple device can appear on all other Apple devices that are associated with the same Apple ID, and have activated the Messages application on that device. An iMessage is sent and received based on an Apple ID, but can also be sent based on the user's telephone number, if a telephone number is associated with that device. If an iMessage is sent, the message uses an Internet data connection, whether that connection is provided by the mobile telephone service provider or a Wi-Fi hotspot. If a data connection is not available to the Apple device, or the Apple device is sending a message to a non-Apple device, the Messages application will default to traditional SMS if possible for delivery of the message. The SUBJECT ACCOUNT would possibly contain the data for iMessage.

9. In my training and experience, evidence of who was using the SUBJECT ACCOUNT may be found in address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Apple. Further, the providers of the SUBJECT ACCOUNT generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name,

19 - 0973 JMC

physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

10. The providers of the SUBJECT ACCOUNT typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

**19 - 0973 JMC**

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used.

13. Additionally, information stored at the SUBJECT ACCOUNT may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offenses under investigation.

14. On May 27, 2016 at approximately 7:20 a.m., Latrina Ashburne was shot and killed in front of her home on Rosalind Ave in Baltimore City (hereinafter “Ashburne murder”). Ms. Ashburne was the next-door neighbor a material witness (“MW”) in the (then) upcoming federal prosecution of Matthew Hightower. Hightower was under federal indictment for both health care fraud charges and extortion charges related to his role in another murder (the September 2013 murder of David Wutoh, hereinafter “Wutoh murder”). Hightower made his initial appearance on the health care fraud charges in June of 2015. Thereafter, the government

**19 - 0973 JMC**

disclosed the MW's name and the substance of her statement to counsel for defendant Hightower as part of the discovery process. Ashburne was similar in age and appearance to the MW and the two women drove similar cars. Ashburne was a pastor at a local church and to date there are no other known suspects with motive to kill her. She was not robbed.

15. Surveillance camera retrieved from the area near the scene of the murder revealed an unknown suspect fleeing the scene on foot. The footage also revealed a 2005 Pontiac Grand Am bearing Maryland tag #BXC31 (hereinafter "Pontiac") close in time and proximity to the fleeing suspect in what appears to investigators to be a getaway vehicle. The Pontiac was traced back to Davon Carter, a longtime and very close associate of Matthew Hightower.

16. The surveillance camera videos also capture a silver Audi with a distinctive long and narrow front license plate. As described further below, investigation has revealed that at that time the Audi belonged to Matthew Hightower. The Audi was in the area near the scene of the murder both before (approximately 6:15 a.m.) and after (approximately 7:30 and 7:55 a.m.). Investigators have since linked the Audi being used at that time to Clifton Mosley, a longtime associate of Matthew Hightower. Mosley was interviewed after he was identified (using call detail records from Davon Carter's phones), however, he denied being in the Audi at the time of the homicide. An analysis of cell site data places Mosley's two phones (including 410-693-1533) in the coverage area of the murder scene at the time of the shooting: 7:20 a.m. Further Mosley and Carter communicated via the 410-693-1533 number in the days leading up to the murder.

17. According to Mosley, he had transferred the Audi to Davon Carter. Mosley said he could not remember the date/time of the transfer. However, cell site data and security cameras likely have Mosley driving the car the morning of May 27 at or about 6:15 a.m. – just as Carter

**19 - 0973 JMC**

was leaving his home. Investigators know that sometime after the homicide on May 27 Carter drove the Audi to Myrtle Beach, South Carolina. This was Memorial Day weekend, and phone records reflect Carter was in the Audi heading south out of Baltimore City no later than 11:00 a.m.

18. Further, evidence establishes that Carter fits the description of the shooter and that immediately after the shooting, the aforementioned Pontiac appeared to be waiting for him immediately after the shooting. Based on the timing of Mosley's arrival near the scene of the murder that morning, his false statements regarding his whereabouts that morning, the gap in his phone usage and other factors, we believe Mosley was driving the same Pontiac that Carter had arrived in to meet with Mosley that morning.

19. On June 1, 2016, Carter was surveilled coming out of his home, going to the Pontiac and then getting in a BMW SUV parked in the same parking lot.

20. Baltimore City homicide detectives interviewed Davon Carter on June 1, 2016, after conducting a traffic stop of the BMW SUV, also registered to Matthew Hightower. During the stop of Carter's car, Detectives recovered approximately two pounds of marijuana and \$7,000 in cash. Investigators subsequently identified drug customers and the source of supply, each of whom testified in grand jury.

21. Mosley admitted in grand jury testimony that he sold marijuana in the 2015-2016 timeframe.

22. At the time that investigators interviewed Carter, they recovered three phones, two of which were "flip" phones – i.e. small, relatively unsophisticated phones without any internet capability. There were very few contacts on these phones. One of the phones had only seven numbers saved in contacts; one was an entry for "Cliff" (Mosley) and the number 410-693-1533.

19 - 0973 JMC

The other phone was an iPhone with telephone number 443-293-2399 that law enforcement had been unable to unlock and search until November 2017.

23. Baltimore City homicide detectives interviewed Davon Carter that day and recorded the interview. Carter never volunteered his interactions with Mosley the night before or the day of the murder. City homicide detectives advised Carter of his *Miranda* warnings and told him the connection of the victim to the federal investigation. He admitted to being in possession of the Pontiac at approximately 7:00 a.m. on May 27, 2016. The shooting occurred at approximately 7:20 a.m. on May 27, 2016. Carter contended, however, that he had dropped the Pontiac off to get new brakes from a guy named "Tony" who did not run a "shop" but hung out in the Park Heights area. Carter did not know or would not provide Tony's last name. Detectives confronted Carter with the fact that the Pontiac was at the scene of the shooting, however, Carter maintained that he had no information about the shooting. He maintained that after he left the car with "Tony," he went to Myrtle Beach for a few days. The police asked how the Pontiac was outside his residence on June 1, 2016 or why he was driving a BMW SUV registered in the name of Matthew Hightower, but Carter did not/could not explain. He admitted that Matthew Hightower was "like family" to him. When asked about the events of Memorial Day Weekend, Carter stated that he went to Myrtle Beach with two of his friends, "Dre" and "Mooch." Investigation has determined that "Dre" is Andre Farrell. Farrell denied driving to Myrtle Beach with Carter and, in fact, his phone records establish that he left the area much earlier on May 27 and arriving in South Carolina no later than 7:25 p.m.

24. The police also interviewed Carter's girlfriend, Deanna Lawson. She stated that Carter left her home at approximately 7:00 a.m. in the Pontiac on May 27, 2016. In fact, Carter's cell site records have him leaving the house no later than 6:15 a.m. She believed he was going to



**19 - 0973 JMC**

Myrtle Beach with “someone named Andre and his brother and his brother’s friend.” According to Lawson, Carter was supposed to drive the Pontiac to meet up with the others to go to Myrtle Beach, not drive the Pontiac to Myrtle Beach. When she returned home from work on Friday May 27 at 3:30 p.m., the Pontiac was in the parking lot. She does not know how the Pontiac got back to her apartment complex on May 27. During a subsequent interview Lawson indicated that, while Carter had left the morning of the murder (May 27, 2016) driving her Pontiac, when he returned from Myrtle Beach several days later Carter was driving the silver Audi with a long tag. Carter told Lawson that the Audi belonged to Matthew Hightower.

25. On December 19, 2017, a Grand Jury in the District of Maryland returned a true bill charging Carter with conspiracy and substantive counts related to murdering a witness, both retaliation, in violation of 18 U.S.C. §1513(a)(1)(B)), and tampering in violation of 18 U.S.C. § 1512(a)(1)(A), for the murder of Latrina Ashburne on May 27, 2016 (hereinafter “the Ashburne murder”). Mosley was indicted as a co-conspirator in the same counts on March 6, 2019. The Indictment also charges Carter and Mosley with drug trafficking offenses.

26. In December 2016, we obtained Mosley’s iPhone, telephone number 410-805-5008, by consent. The forensic data for the phone associates the account with Apple ID nyree08@icloud.com. The forensic data contains information regarding communications Mosley had as early as March 2016 through December but there are apparent gaps which may be the result of the fact that the device he had in December 2016 imported information from Mosley’s device/number that he used in May 2016 which is 410-693-1533. In other words, the SUBJECT ACCOUNT may contain the “backup” data for the 410-693-1533 number.

27. Mosley’s whereabouts, his communications leading up to the murder, as well as after, are integral to proving his motive, the lack of alibi, and identifying other associates

19 - 0973 JMC

possibly involved. Hence, there is probable cause to believe that the SUBJECT ACCOUNT will contain information relevant to the ongoing investigation into the TARGET OFFENSES.

28. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

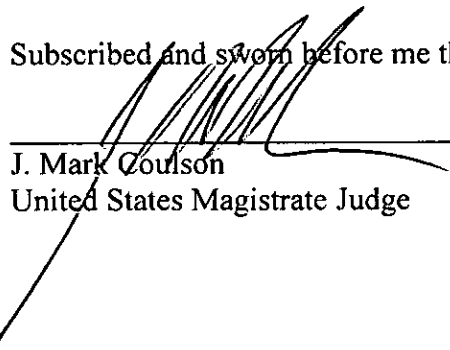
**CONCLUSION**

29. Based on the facts set forth above, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the violations of the above-enumerated offenses are presently on the SUBJECT ACCOUNT further described in Attachment A, which are to be searched for the items listed in Attachment B.

46. I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.

  
Special Agent Erin Fuchs  
United States Department of Health and Human Services

Subscribed and sworn before me this 22 day of March, 2019

  
J. Mark Coulson  
United States Magistrate Judge



SW